

RECEIVED
CENTRAL FAX CENTER

OCT 24 2005

2910-101

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of) BEFORE THE BOARD OF PATENT
Noriaki Hashimoto) APPEALS AND INTERFERENCES
Serial No. 09/690,818)
Filed: 10/18/2000)
For: METHOD AND SYSTEM FOR)
PREVENTING UNAUTHORIZED) October 24, 2005
ACCESS TO A NETWORK) (Monday)

BRIEF ON APPEAL

Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

This is an appeal from the final rejection of claims 1 to 23 of the above-identified application, which claims were finally rejected in the Office action dated January 27, 2005. A Notice of Appeal was timely filed on June 22, 2005. A Petition for Extension of time for filing the Brief on Appeal is attached hereto.

REAL PARTY IN INTEREST

The real party in interest in this case is the inventor, Mr. Noriaki Hashimoto.

10/26/2005 CNGUYEN 00000039 141437 09690818
01 FC:2402 250.00 DA

Serial No. 09/690,818

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences which will directly affect or be directly affected by or have a bearing on the Board's decision in the present appeal.

STATUS OF THE CLAIMS

Claims 1 to 23 are pending in the application. Claims 1 to 23 have been rejected. This appeal is directed to all of the rejected claims 1 to 23.

STATUS OF AMENDMENTS

The status of amendments is as set forth in the Response filed on June 22, 2005. In that regard, claims 1 to 15, 17 to 20 and 22 to 23 are the same as that originally filed (i.e., original claims), and claims 16 and 21 were previously amended in the Amendment filed on August 19, 2004.

Serial No. 09/690,818

SUMMARY OF THE CLAIMED SUBJECT MATTER

The present invention relates to systems and methods for preventing unauthorized access to a computer network (e.g., to the Internet). In this regard, when a user desires to connect to a network, such as, e.g., the Internet, via the user's user computer (such as, e.g., a personal computer at which a user accesses the Internet using browser software running on their computer), the user typically seeks to connect to the Internet via a host computer (such as, e.g., a server of an Internet service provider like AOL or the like). In effecting such a connection, the user computer has an IP address which is assigned to that user computer (e.g., which can be a permanent IP address or a dynamically assigned IP address). Previously, there was a risk that computer hackers and malicious users could seek to gain inappropriate access to networks by using an IP address without authorization. This problem existed because IP addresses were usable without regard to whether there was a match between an IP address and a proper IP address *assigned to that user computer*.

Now, with the present invention, unauthorized access can be prevented by allowing access only when an IP address of a data packet received from a user computer matches an IP address *assigned to that user computer*.

Serial No. 09/690,818

As explained in the very first paragraph of the Summary of the Invention, "the present invention is directed to a method and system for preventing an access to a network **when an originating IP address of a data packet does not match the IP address assigned to that computer.**" See Summary of the Invention, page 4, lines 16 to 18 (emphasis added).

In order to carry out embodiments of the present invention, a correlation is specifically made between an IP address and a particular user computer (i.e., the user computer and the IP address must both be correlated so as to effect such a correlation, such that access can be granted or denied to the user computer based on an IP addressed **assigned to that user computer**).

Independent Claim 1

The subject matter to which independent claim 1 relates involves an access control system for preventing an unauthorized access to a network via a user computer connected to the network. "With reference to FIG. 1, one embodiment of a secure network using access control systems ... includes a user computer 100 connected to a host computer system 102 via [a] Public Switched Telephone Network (PSTN) 101." See page 8, lines 18 to 20. "An access control system [e.g., 102E, 102F and 102G] is [in some embodiments]

Serial No. 09/690,818

located within or close to the host computer system 102, so that a user has no physical access to it." See page 9, lines 4 to 13. As explained on page 9, lines 16 to 21:

[T]he access control system 102E would contain the IP address ***assigned to the user computer*** 100 and would monitor data packets sent from the user computer 100. When the stored IP address does not match an originating IP address of a data packet received from the user computer 100 via the modem 102B, the access control system 102E would terminate the connection between the user computer 100 and the host computer system 102. Emphasis added for reference.

Claim 1 recites a number of features related to the access control system. In this regard, some illustrative components of an access control system are discussed at page 10, lines 11 to 17 and shown in FIG. 4. Among other things, the access control system includes a memory (e.g., 400A) containing an IP address ***assigned to the user computer***, and a microprocessor (e.g., 400B) programmed to terminate a connection between the user computer and the network when an originating IP address of a data packet received from the user computer (e.g., 401) does not match the IP address ***assigned to the user computer*** (e.g., 401) that is contained in the memory.

"Typically, an IP address is ***assigned to the user computer*** 401 by the host computer system 402 when the connection between the user computer 401 and the host computer system 402 is established." See page 11 lines 18 to 20

Serial No. 09/690,818

(emphasis added). As explained at page 11, lines 7 to 10: "If an IP address to the user computer 401 is dynamically assigned, the memory 400A is updated when a new IP address is **assigned to the user computer 401**. If the user computer 401 has a permanent IP address, the memory 400A contains that address."

FIG. 6 shows another embodiment of an access control system, including a memory, a comparative structure with a comparator 602 and an AND gate 602. The memory 600 contains IP addresses **assigned to the user computers** connected to the access control system. See page 12, lines 4 to 12.

FIG. 5 demonstrates the operation of an access control system. As shown, "[a]t step 500, an IP address **assigned to a user computer** is stored in the memory of the access control system." See page 12, lines 14 to 15 (emphasis added). Then, "[a]t steps 501 and 502, an originating IP address of a data packet received from the user computer is compared with the **IP address of the user computer** stored in the memory." See page 12, line 21 to page 13, line 1 (emphasis added). "If the two IP addresses are the same, the data packet is sent to a network, which typically is the Internet, at step 503." See page 13, lines 1 to 3. "If the two IP addresses do not match, the access control system causes

Serial No. 09/690,818

a connection between the user computer and the host computer system to terminate at step 504." See page 13, lines 4 to 6.

FIG. 2 depicts another embodiment of a secure network using access control systems of the present invention, in which, e.g., a host computer system includes a hub 202A and access control systems 202B and 202C.

FIG. 3 depicts yet another embodiment of a secure network using access control systems of the present invention, in which, e.g., access control systems 303, 304, 305 are located between user computers and an access server 306. In some embodiments, the access control systems are located near the user computers (in which cases, e.g., capabilities to detect a physical tampering may be desired), such that users can have physical access to them or can be located distant to such user computers. In some embodiments, "[e]ach access control system is responsible for monitoring an originating IP address of each data packet sent from a user computer connected to it." See page 15, lines 13 to 15.

Independent Claim 5

Claim 5 relates to subject matter having general similarity to the subject matter to which claim 1 relates. In this regard, claim 5 relates to an access

Serial No. 09/690,818

control system for preventing an unauthorized access to a network via a user computer (e.g., 100, 401) connected to the network through a host computer system (e.g., 102, 402). Claim 5 includes a memory (e.g., 400A) containing an IP address assigned to the user computer, and a microprocessor (e.g., 400B) programmed to terminate a connection between the user computer and the host computer system when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory. In addition, independent claim 5 also relates to embodiments in which the access control system is located between the user computer and the host computer system.

Independent Claim 9

Claim 9 relates to subject matter having general similarity to the subject matter to which claim 1 relates. In this regard, claim 9 relates to a method for preventing an unauthorized access to a network via a user computer (e.g., 100, 401) which is connected to the network and to an access control system (e.g., 102E-102G, 400). The method includes storing an IP address of the user computer in a memory (e.g., 400A) of the access control system, receiving a data packet from the user computer (e.g., 100, 401A), comparing an originating IP address of the data packet with the IP address of the user computer stored in the

Serial No. 09/690,818

memory (e.g., 400A) of the access control system, and denying the user computer an access to the network (e.g., 103, 307, 402) if the originating IP address of the data packet is different from the IP address of the user computer (e.g., 100, 200-201, 401) stored in the memory (e.g., 400A) of the access control system (e.g., 102E-102G, 400).

Independent Claim 13

Claim 13 relates to subject matter having general similarity to the subject matter to which claim 1 relates. In this regard, claim 13 relates to a method of preventing an unauthorized access to a network via a user computer (e.g., 100, 200-201, 401) connected to the network through a host computer system (e.g., 102, 402) which is connected to an access control system (e.g., 400). The method includes storing an IP address of the user computer in a memory (e.g., 400A) of the access control system, receiving a data packet from the user computer (e.g., 100, 200-201, 401), comparing an originating IP address of the data packet with the IP address of the user computer stored in the memory of the access control system (see, e.g., microprocessor 400B and page 10, line 21 to page 11, line 2), and terminating a connection between the user computer and the host computer system if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory of the

Serial No. 09/690,818

access control system (see, e.g., page 11, lines 2 to 10).

Independent Claim 16

Claim 16 relates to subject matter having general similarity to the subject matter to which claim 1 relates. In this regard, claim 16 relates to a secure network that includes: a host computer system (e.g., 102, 402) connected to the secure network, an access control system (e.g., 102E-102G, 202B-202C, 303-305, 400) connected to the host computer system and having a memory (e.g., 400A), a user computer (e.g., 100, 401) connected to the host computer system (e.g., 102, 402) and configured to access the secure network (e.g., 103) through the host computer system, wherein the memory (e.g., 400A) of the access control system is programmed to terminate a connection between the host computer system and the user computer when an originating IP address of a data packet sent from the user computer for transmission to a node in the secure network does not match the IP address of the user computer (e.g., 100, 401) contained in the memory of the access control system.

Independent Claim 20

Claim 20 relates to subject matter having general similarity to the subject

Serial No. 09/690,818

matter to which claim 1 relates. In this regard, claim 20 relates to a secure network that includes: a user computer system (e.g., 100, 401) connected to the secure network, an access control system (e.g., 102E-102G, 202B-202C, 303-305, 400) connected to the user computer and having a memory (e.g., 400A), wherein the memory of the access control system contains an IP address assigned to the user computer (e.g., 100, 401), and wherein the access control system is programmed to deny the user computer an access to the secure network when an originating IP address of a data packet sent from the user computer for transmission to a node in the secure network does not match the IP address of the user computer contained in the memory of the access control system.

Independent Claim 21

Claim 21 relates to subject matter having general similarity to the subject matter to which claim 1 relates. In this regard, claim 21 relates to an access control system for preventing an unauthorized access to a network (e.g., Internet 103) via a user computer (e.g., 100, 401) connected to the network, including a memory (e.g., 400A) containing an IP address assigned to the user computer; and a comparator structure (see FIG. 6 and comparator 602) configured to terminate a connection between the user computer and the network when an

Serial No. 09/690,818

originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory. See, e.g., page 12, lines 4 to 12.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

This appeal presents the following issues for review by the Board:

- 1) Whether claims 9 and 11 to 12 are unpatentable under 35 U.S.C. § 102(e) as being anticipated by Maria, et al., U.S. Patent Publication No. US2004/0073671 ("Maria"), and are properly rejected on that basis; and

- 2) Whether claims 1 to 8, 10 and 13 to 23 are unpatentable under 35 U.S.C. § 103 as being obvious over Maria, et al., U.S. Patent Publication No. US2004/0073671 ("Maria"), and are properly rejected on that basis.

Serial No. 09/690,818

ARGUMENT**I.****INTRODUCTORY COMMENTS REGARDING THE MARIA REFERENCE**

It is respectfully submitted that the Maria reference has substantial deficiencies that were improperly overlooked by the Patent Examiner. It is most respectfully requested that the Board carefully review the Maria reference. For the Board's understanding, some introductory comments regarding the Maria reference are now provided.

1. The Maria Reference Has the Same Problems as Found In the Background Art Described In the Present Application Which The Present Invention Seeks to Overcome

As described in the present application in the Discussion of the Related Art, a notable problem with the background art involved that there was previously no way to prevent computer hackers or malicious users from improperly altering their IP addresses and, thus, from conducting malicious acts over the Internet or the like.

Despite serious economic damages caused by malicious acts over the Internet, efforts by business and government institutions to detect and

Serial No. 09/690,818

prevent such acts have not been very effective. This is partly due to the difficulty in tracing identities of those who commit malicious acts over the Internet. ... For example, it is often difficult to identify individual[s] responsible for committing malicious acts because they can hide their identities relatively easily Specifically, one can hide his or her identity by [e.g.] altering IP addresses of data packets

In particular, it is important to prevent an access to the Internet by those who try to mask their identities by **altering an originating IP address** of a data packet they send.

See the present application Discussion of the Related Art at page 3, lines 8 to 16 (emphasis added), page 4, lines 1 to 3 (emphasis added), and page 4, lines 8 to 10 (emphasis added).

Despite these specifically identified problems in the background art, the Maria reference relied upon in the Office Action has these same problems and does not provide any means to address the problem of malicious attackers **altering their originating IP addresses**.

With the Maria technology, as long as a correct IP address is provided, the data packet transmission is passed through. The Maria technology has **no mechanisms to prevent** malicious attackers from improper use of the IP addresses of other parties.

Thus, the Maria reference merely continues to have the same types of problems as sought to be overcome by the present invention.

Serial No. 09/690,818

A. Filtering Based On Large List of Approved Site IP Addresses

As set forth above, with the Maria reference, as long as a designated IP address is contained on an approved IP address list, the transmission will be approved. There is no means to ascertain if the transmission includes a correct IP address *for a particular user computer.*

In this regard, the Maria reference merely focuses on "filtering" of Internet Web Site "content" that is provided to users over the Internet. In order to do so, the reference teaches the maintaining of a large list of approved site IP addresses so as to restrict content received over the Internet.

The reference explains that "[w]ith the growing number of Internet sites, there is ... a growing number of sites which provide content that some companies may deem inappropriate." See column 1, lines 23+ (emphasis added). In this context, the Maria reference indicates that "a substantial need exists for a ... data packet filter which can work with a large number of source IP addresses." See column 2, lines 30+.

Toward that end, the Maria reference "proposes a ... filtering processor

Serial No. 09/690,818

whose **only function** is to filter data packets based on a list of source IP addresses." See column 2, lines 37+ (emphasis added). Here, the reference explains that "the central administrator ... obtains new source IP address information from various sources, such as service providers or search robots specializing in gathering source IP addresses by category, e.g., telemarketers, adult material, advertising entities, hate groups, and so forth." See column 2, lines 22+. The reference explains that this "list of source IP addresses" "rang[es] from hundreds to several thousand." See column 4, lines 35+.

Thus, the Maria reference merely teaches that the system operates such that a "packet is passed if the source IP address does match an address from list 33, and is dropped otherwise." See column 6, lines 39+. That is, the system passes the packet if it is from any one from a long list of IP Addresses. See also column 2, lines 42+ (emphasis added).

Once again, with the Maria reference, as long as a designated IP address is contained on the approved IP address list, the transmission will be approved. There is no means to ascertain if the transmission includes a correct IP address *for a particular user computer.*

Serial No. 09/690,818

B. IP Address Filtering Without Regard To Source Computer Identity

As expressed above, the Maria reference maintains this list of IP addresses without regard to what computer may use such IP addresses. In this regard, the IP addresses for Internet Web Sites can be implemented by various computers and can be switched to new computers. By way of example, a Web Site can potentially be switched to a new service provider having new computers at new locations, but utilizing the same IP addresses of the Web Site.

The Maria reference does not involve any matching or the like of such IP addresses to computers.

C. No Security Provided Against "Unauthorized" Use of IP Addresses

The Maria reference relates to "filtering" of Internet Web Site "content." The Maria reference does not address whether there is any "authorization" to receive communications from a user of a certain IP address and is not concerned with protecting against unauthorized use of IP addresses.

As previously noted, on the other hand, with the present invention, untraceable malicious acts can be prevented and those responsible for such acts

Serial No. 09/690,818

can be caught. The present invention can, inter alia, prevent individuals from accessing a network when they alter IP addresses of data packets. For example, exemplary acts of attacking based on the unauthorized use of IP addresses (such as, e.g., common attacks known as "IP-spoofing" attacks, smurf attacks, teardrop attacks, etc.) can be prevented

The Maria reference is **wholly incapable** of addressing these sorts of activities in which an attacker makes improper use of an IP address.

II.

INTRODUCTORY REMARKS REGARDING EXAMINER'S CLAIM INTERPRETATIONS

In paragraph 2.1 of the Final Office Action, the Examiner indicates that "Maria discloses the storing of user IP address, the comparing with the stored IP address and the denying/restricting access based on the comparing." It is most respectfully submitted that the Examiner appears to misunderstand that IP addresses are **independent** of a particular computer. Thus, the action of "storing" and "comparing" identified by the Examiner do **not** encompass **assigning of an IP address to a particular used computer.**

Serial No. 09/690,818

It is most respectfully submitted that the Examiner has wrongly identified features on which Applicant relies as being a "determination of when the user computer has altered its IP address from the IP address assigned." Among other things, the Maria reference does not teach or suggest the assigning of an IP address to a particular computer, the storing of such an assignment in a memory, nor the prevention of unauthorized access based on such an assignment. It is respectfully submitted that the claims recite other limitations that are not even remotely suggested by the Maria reference, which features are being improperly discarded by the Examiner. Careful consideration of the following remarks is respectfully requested.

III.

THE REJECTIONS OF CLAIMS 1 TO 8, 10 AND 13 TO 23 ARE IMPROPER

It is most respectfully submitted that the rejections of claims 1 to 8, 10 and 13 to 23 under 35 U.S.C. § 103 are improper and should be reversed.

A. Independent Claim 1

1. Claim Limitations Not Taught or Suggested

Among other things, claim 1 recites:

Serial No. 09/690,818

"a microprocessor programmed to terminate a connection between the user computer and the network when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory."

The Maria reference does not even remotely teach or suggest such features. The following sections discuss some of these and other deficiencies in further detail.

a. **No Match to Computer**

Among other things, the above-identified recitations in claim 1 include having an "IP address **assigned to the user computer.**" Emphasis added. On the other hand, the Maria reference does not involve having any IP Address being assigned to any computer. As set forth above, the IP addresses in the Maria reference are listed without regard to the identity of a source computer.

As explained above, the Maria system merely passes packets as long as they are from any one of a long list of IP Addresses, see e.g. column 2, lines 42+, without any regard for whether or not a particular source computer transmits a packet having a particular IP Address.

Serial No. 09/690,818

b. **No Termination Without Match**

Among other things, the above-noted recitations in claim 1 also include that there is a "microprocessor programmed to terminate a connection ... when an originating IP address ... ***does not match the IP address assigned to the user computer.***" It is most respectfully submitted that the Maria reference cannot be reasonably construed to include such features.

Notably, the Maria reference maintains a large source list of IP Addresses – i.e., which includes "hundreds to several thousand" IP Addresses. See column 4, lines 34 to 36 of the Maria reference. Accordingly, the Maria reference will not "terminate a connection" under the conditions recited in claim 1. Notably, since the source list includes hundreds or thousands IP Addresses, which relate to hundreds or thousands of computers, the Maria reference will necessarily allow the communication and will clearly allow the connection under many situations in which "an originating IP address ... does not match [an] IP address assigned to the user computer," rather than terminating the connection.

c. **No Prevention of Unauthorized Access Via That User Computer**

In addition to the foregoing, it is noted that claim 1 is directed to "[a]n

Serial No. 09/690,818

access control system for preventing an unauthorized access to a network via a user computer." On the other hand, the Maria reference does not contemplate what identity a source computer may have, much less how to prevent unauthorized access via such a computer.

2. Examiner's Incorrect Interpretation

It is also respectfully submitted that the Examiner has incorrectly identified paragraph 0008 as somehow teaching "storing an IP address **assigned to the user computer** in a memory of the access control system." Emphasis added. In contradistinction, the Maria reference merely teaches the storing of a large list of IP addresses, without any regarding to assignment to a particular user computer. It is respectfully submitted that this distinction cannot be improperly overlooked because such a distinction is expressly claimed and has very substantial results achieved therefrom – i.e., the ability to "deny the user computer an access" under the specific conditions noted in the claim.

3. Examiner's Improper Modification of the Maria Reference

In paragraph 4.2, the Examiner indicates that "it would have been obvious to ... modify the method or system of Maria et al. to terminate the connection

Serial No. 09/690,818

between the user computer and the host computer." However, in Maria the system and method relates to controlling the flow of packets to a user. Rather than addressing access to a host computer by a user computer, the Maria reference relates to filtering of packets delivered to a user. The Maria reference, thus, is intended so as to allow numerous communications to pass through (e.g., from lists of thousands of source IP addresses) and to filter out or prevent only that which is not on the approved list. It would make no sense to modify the Maria reference to alter this functionality so as to "terminate" the users connection upon the occurrence of an item not on the approved list. Such a modification would fundamentally change the intended operation of the Maria device as a filter in which some items are "approved" and others are "not approved" since the Examiner's proposal would essentially terminate the entire process upon receiving a packet that is "not approved."

In addition, the Examiner expresses that "[t]he process of terminating a connection between a user and a host is well known in the art." While terminating a connection of a user and a host is, of course, known in some contexts, such as, e.g., when one logs out of their AOL dial-up connection over the internet, the bases or the reasons for terminations in the context of the present invention is clearly not even remotely suggested in the art.

Serial No. 09/690,818

B. Independent Claim 5

Among other things, claim 5 recites:

"a microprocessor programmed to terminate a connection between the user computer and the host computer system when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory" Emphasis added for reference.

Parallel to the discussion above with reference to claim 1, the Maria reference does not even remotely teach or suggest the combination of features recited in claim 5, including, e.g., the limitations identified and highlighted above.

C. Independent Claim 13

Among other things, claim 13 recites:

"terminating a connection between the user computer and the host computer system if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory of the access control system." Emphasis added for reference.

Parallel to the discussion above with reference to claim 1, the Maria reference does not even remotely teach or suggest the combination of features recited in claim 13, including, e.g., the limitations identified and highlighted above.

Serial No. 09/690,818

D. Independent Claim 16

Among other things, claim 16 recites:

"the access control system is programmed to terminate a connection between the host computer system and the user computer when an originating IP address of a data packet sent from the user computer for transmission to a node in the secure network does not match the IP address of the user computer contained in the memory of the access control system." Emphasis added for reference.

Parallel to the discussion above with reference to claim 1, the Maria reference does not even remotely teach or suggest the combination of features recited in claim 16, including, e.g., the limitations identified and highlighted above.

E. Independent Claim 20

Among other things, claim 20 recites:

"the access control system is programmed to deny the user computer an access to the secure network when an originating IP address of a data packet sent from the user computer for transmission to a node in the secure network does not match the IP address of the user computer contained in the memory of the access control system." Emphasis added for reference.

Parallel to the discussion above with reference to claim 1, the Maria

Serial No. 09/690,818

reference does not even remotely teach or suggest the combination of features recited in claim 20, including, e.g., the limitations identified and highlighted above.

F. Independent Claim 21

Among other things, claim 21 recites:

"a comparator structure configured to terminate a connection between the user computer and the network when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory." Emphasis added for reference.

Parallel to the discussion above with reference to claim 1, the Maria reference does not even remotely teach or suggest the combination of features recited in claim 21, including, e.g., the limitations identified and highlighted above.

IV.

THE REJECTIONS OF CLAIMS 9 AND 11-12 ARE IMPROPER

The rejection of claims 9 and 11 to 12 under 35 U.S.C. § 102 are improper and should be reversed.

Serial No. 09/690,818

A. Independent Claim 9

Among other things, claim 9 recites:

"denying the user computer an access to the network if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory of the access control system."
Emphasis added for reference.

Parallel to the discussion above with reference to claim 1, the Maria reference does not even remotely teach or suggest the combination of features recited in claim 9, including, e.g., the limitations identified and highlighted above.

As indicated above, it is respectfully submitted that the Examiner has incorrectly identified paragraph 0008 as somehow teaching "storing an IP address **assigned to the user computer** in a memory of the access control system." In contradistinction, the Maria reference merely teaches the storing of a large list of IP addresses, without any regarding to assignment to a particular user computer. It is respectfully submitted that this distinction cannot be improperly overlooked because such a distinction is expressly claimed and has very substantial results achieved therefrom – i.e., the ability to "deny the user computer an access" under the specific conditions noted in the claim.

Serial No. 09/690,818

V.
REJECTIONS OF THE DEPENDENT CLAIMS

In addition to the rejections of the independent claims, as discussed above, it is respectfully submitted that the Patent Office has improperly disregarded features recited in each of the dependent claims. Independent consideration of each of the dependent claims is most respectfully requested.

A. Dependent Claims 2, 6, 12 and 14

It is respectfully submitted that the Maria reference does not teach the combinations of features recited in claim 2 including "wherein the microprocessor is further programmed to delete the IP address of the user computer from the memory *when the originating IP address of the data packet received from user computer does not match the IP address assigned to the user computer that is contained in the memory.*"

The paragraph [0044] identified by the Examiner does not teach such programming for deletion of the IP address. In contradistinction, the reference describes in paragraphs [0043] to [0045] very different mechanisms for modification of the list. This makes complete sense too because, after all, the purposes of the list in the Maria reference is totally different. In the Maria

Serial No. 09/690,818

reference, “[i]n accordance with the system administration aspects of the invention, a service provider administers a database of source IP address lists.” See paragraph [0043]. In the Maria system, it would make no sense to “delete” the IP address from a list when there is no match because if there is no match it is necessarily NOT on the list already. That is because the Maria reference does not have a list of IP addresses assigned to computers, so there is no means to make such an identification. This rejection is wholly improper.

Claims 6, 12 and 14 also recite features related to, e.g., deleting the IP address of the user computer from the memory and should, thus, also recite combinations of features that are further not taught or suggested by the references.

B. Dependent Claims 3, 7, 11 and 15

It is respectfully submitted that the Maria reference does not teach the combinations of features recited in claim 3 including “wherein the microprocessor is further programmed to update the IP address of the user computer contained in the memory.” Emphasis added.

In this regard, because the Maria reference does not even have any

Serial No. 09/690,818

designation of an IP address for a particular user computer, it makes no sense that such an IP address would be "updated." In addition, the Maria reference does not contemplate any ability to update such IP addresses on a per computer basis. Paragraph [0044] cited by the Examiner in no way relates to any such features.

Claims 7, 11 and 15 also recite features related to, e.g., updating the IP address of the user computer stored in the memory, and, thus, also recite combinations of features that are further not taught or suggested by the references.

C. Dependent Claim 10

It is respectfully submitted that the Maria reference does not teach the combinations of features recited in claim 10, including "wherein the denying step includes terminating the connection between the user computer and the network." In this regard, as discussed above with reference to claim 1, it is most respectfully submitted that the Maria reference merely relates to the filtering of packets that are delivered to a user, and it, thus, makes no sense to for some reason terminate such a connection in Maria because it would, thus, defeat the purpose of allowing some appropriate content through and not allowing other

Serial No. 09/690,818

content through as a filter.

D. Dependent Claim 18

It is respectfully submitted that the Maria reference does not teach the combinations of features recited in claim 18, "wherein the host computer system comprises an access server and a plurality of modems and wherein the access control system is located between the access server and the plurality of modems." In this regard, it is most respectfully submitted that the Maria reference does not teach or suggest that an access control system, as claimed, would be located specifically between the access server and the plurality of modems. It is respectfully submitted that the Examiner's statements that "[i]t obvious to one skilled in the art that the disclosure of Maria meets the recitations" claimed is incorrect.

CONCLUSION

In view of the foregoing, claims 1 to 23 are submitted to be directed to a new and unobvious systems and methods for preventing unauthorized access to a network, which are not taught by the prior art. The Honorable Board is respectfully requested to reverse all grounds of rejection and to direct the passage of this application to issue.

Serial No. 09/690,818

Please charge any fee or credit any overpayment pursuant to 37 CFR
1.16 or 1.17 to Deposit Account No. 14-1437.

Respectfully submitted,
Watchstone P+D,
an affiliate of Novak, Druce, DeLuca & Quigg

By _____


Stephen B. Parker
Attorney for Appellant
Registration No. 36,631

1300 Eye Street, N.W.
Suite 400 East Tower
Washington, D.C. 20005
Telephone: (202)659-0100

I hereby certify that this document is being facsimile transmitted to the USPTO at 571-273-8300 or deposited with the US Postal Service with sufficient postage as first class mail in an envelop addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on October 24, 2005.

Name: Stephen B. Parker


Signed.

Serial No. 09/690,818

APPENDIX OF CLAIMS ON APPEAL

1. An access control system for preventing an unauthorized access to a network via a user computer connected to the network, the system comprising;
 - a memory containing an IP address assigned to the user computer; and
 - a microprocessor programmed to terminate a connection between the user computer and the network when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory.
2. The access control system of claim 1, wherein the microprocessor is further programmed to delete the IP address of the user computer from the memory when the originating IP address of the data packet received from user computer does not match the IP address assigned to the user computer that is contained in the memory.
3. The access control system of claim 1, wherein the microprocessor is further programmed to update the IP address of the user computer contained in the memory.

Serial No. 09/690,818

4. The access control system of claim 1, wherein the memory is a part of the microprocessor.

5. An access control system for preventing an unauthorized access to a network via a user computer connected to the network through a host computer system, the system comprising:

a memory containing an IP address assigned to the user computer; and
a microprocessor programmed to terminate a connection between the user computer and the host computer system when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory,

wherein the access control system is located between the user computer and the host computer system.

6. The access control system of claim 5, wherein the microprocessor is further programmed to delete the IP address of the user computer from the memory when the originating IP address of the data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory.

Serial No. 09/690,818

7. The access control system of claim 5, wherein the microprocessor is further programmed to update the IP address of the user computer contained in the memory.

8. The access control system of claim 5, wherein the memory is a part of the microprocessor.

9. A method for preventing an unauthorized access to a network via a user computer which is connected to the network and to an access control system, the method comprising:

storing an IP address of the user computer in a memory of the access control system;

receiving a data packet from the user computer;

comparing an originating IP address of the data packet with the IP address of the user computer stored in the memory of the access control system;
and

denying the user computer an access to the network if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory of the access control system.

Serial No. 09/690,818

10. The method of claim 9, wherein the denying step includes terminating the connection between the user computer and the network.

11. The method of claim 9, further comprising updating the IP address of the user computer stored in the memory of the access control system.

12. The method of claim 9, further comprising deleting the IP address of the user computer from the memory of the access control system if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory of the access control system.

13. A method of preventing an unauthorized access to a network via a user computer connected to the network through a host computer system which is connected to an access control system, the method comprising:

storing an IP address of the user computer in a memory of the access control system;

receiving a data packet from the user computer;

comparing an originating IP address of the data packet with the IP address of the user computer stored in the memory of the access control system; and

terminating a connection between the user computer and the host

Serial No. 09/690,818

computer system if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory of the access control system.

14. The method of claim 13, further comprising deleting the IP address of the user computer from the memory of the access control system if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory of the access control system.

15. The method of claim 13, further comprising updating the IP address of the user computer stored in the memory of the access control system.

16. A secure network comprising:
a host computer system connected to the secure network;
an access control system connected to the host computer system and having a memory; and
a user computer connected to the host computer system and configured to access the secure network through the host computer system,
wherein the memory of the access control system is programmed to terminate a connection between the host computer system and the user computer when an originating IP address of a data packet sent from the user

Serial No. 09/690,818

computer for transmission to a node in the secure network does not match the IP address of the user computer contained in the memory of the access control system.

17. The secure network of claim 16, wherein the user computer and the host computer system are connected via a Public Switched Telephone Network.

18. The secure network of claim 16, wherein the host computer system comprises an access server and a plurality of modems and wherein the access control system is located between the access server and the plurality of modems.

19. The secure network of claim 16, wherein the host computer system and the user computer are connected via a local area network.

20. A secure network comprising:
a user computer connected to the secure network; and
an access control system connected to the user computer and having a memory,

wherein the memory of the access control system contains an IP address assigned to the user computer, and wherein the access control system is programmed to deny the user computer an access to the secure network when

Serial No. 09/690,818

an originating IP address of a data packet sent from the user computer for transmission to a node in the secure network does not match the IP address of the user computer contained in the memory of the access control system.

21. An access control system for preventing an unauthorized access to a network via a user computer connected to the network, the system comprising:

a memory containing an IP address assigned to the user computer; and
a comparator structure configured to terminate a connection between the user computer and the network when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory.

22. The access control system of claim 21, wherein a comparator structure comprises a microprocessor.

23. The access control system of claim 22, wherein the memory is a part of the microprocessor.